Mémo : Commandes Cisco IOS (Switch & Routeur)

Documentation rédigée par : GADONNAUD Ewen

Formation : BTS SIO 1ère année - Option SISR

Établissement : Lycée Paul-Louis Courier, Tours

Date : Mars 2026

1. Navigation et modes

Toutes les commandes sont en mode privilégié (`enable`) sauf mention contraire. Le symbole `#` indique le mode privilégié, `(config)#` le mode configuration globale.

```
enable                          ! Passe en mode privilégié
configure terminal              ! Passe en mode configuration globale
exit                            ! Remonte d'un niveau
end                             ! Retourne directement en mode privilégié
Ctrl+Z                          ! Équivalent à end
```

Sauvegarder la configuration

```
copy running-config startup-config   ! Sauvegarde la config active
write memory                         ! Équivalent court
show running-config                  ! Affiche la config active
show startup-config                  ! Affiche la config sauvegardée
```

2. Informations et diagnostic

```
show version                         ! Version IOS, uptime, modèle
show interfaces                      ! État de toutes les interfaces
show interfaces GigabitEthernet0/0   ! Détail d'une interface
show ip interface brief              ! Résumé IP de toutes les interfaces
```

```
show ip route                          ! Table de routage
show arp                               ! Table ARP
show mac address-table                 ! Table MAC (switch)
show vlan brief                        ! Résumé des VLANs (switch)
show spanning-tree                     ! État du STP
show cdp neighbors                     ! Voisins Cisco détectés
ping 192.168.1.1                       ! Test de connectivité
traceroute 192.168.1.1                 ! Tracé de route
```

3. Configuration des interfaces

Interface routeur

```
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 description LAN Principal
 no shutdown                           ! Active l'interface
 shutdown                              ! Désactive l'interface
```

Interface switch (accès)

```
interface FastEthernet0/1
 description Poste-Utilisateur
 switchport mode access
 switchport access vlan 10
 no shutdown
```

Plage d'interfaces

```
interface range FastEthernet0/1-12
 switchport mode access
 switchport access vlan 10
 no shutdown
```

4. VLANs

Créer et nommer un VLAN

```
vlan 10
 name USERS
vlan 20
 name SERVEURS
vlan 30
 name MANAGEMENT
```

Assigner un port en mode access

```
interface FastEthernet0/1
 switchport mode access
 switchport access vlan 10
```

Configurer un port trunk

```
interface GigabitEthernet0/1
 switchport mode trunk
 switchport trunk encapsulation dot1q      ! Nécessaire sur certains
switches
 switchport trunk allowed vlan 10,20,30    ! Restreindre les VLANs autorisés
 switchport trunk native vlan 99           ! VLAN natif (non taggué)
```

Vérification

```
show vlan brief
show interfaces trunk
show interfaces FastEthernet0/1 switchport
```

5. Sous-interfaces (Router-on-a-Stick)

Configuration du routage inter-VLAN sur une seule interface physique :

```
interface GigabitEthernet0/0
 no shutdown

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 description Gateway-VLAN10

interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 description Gateway-VLAN20

interface GigabitEthernet0/0.99
 encapsulation dot1Q 99 native
 description VLAN-Natif
```

6. VTP (VLAN Trunking Protocol)

VTP permet de propager automatiquement les VLANs entre switches via les liens trunk.

Mode	Rôle
Server	Crée, modifie et supprime les VLANs. Propage les infos.
Client	Reçoit et applique les VLANs du serveur. Ne peut pas créer de VLANs.
Transparent	N'applique pas VTP mais propage les messages. VLANs locaux uniquement.

Configuration VTP

```
vtp mode server                          ! ou client / transparent
vtp domain NOM_DOMAINE                   ! Même domaine sur tous les switches
vtp password motdepasse                  ! Optionnel mais recommandé
vtp version 2                            ! Version 2 recommandée
```

Vérification

```
show vtp status
show vtp password
```

Un switch en mode Server avec un numéro de révision VTP plus élevé peut écraser la base de VLANs de tout le domaine. Toujours remettre le numéro de révision à 0 avant d'intégrer un switch dans un domaine existant (passer en transparent puis en client/server).

7. Routage statique

```
ip route 192.168.2.0 255.255.255.0 192.168.1.254    ! Route statique
ip route 0.0.0.0 0.0.0.0 203.0.113.1                ! Route par défaut
```

Vérification

```
show ip route
show ip route static
```

8. ACL (Access Control Lists)

Les ACL filtrent le trafic sur la base de critères (IP source, destination, protocole...).

Type	Numéros	Critères
Standard	1-99 / 1300-1999	IP source uniquement
Étendue	100-199 / 2000-2699	IP src/dst, protocole, port

ACL Standard (nommée)

```
ip access-list standard BLOC-VLAN30
```

```
 deny   192.168.30.0 0.0.0.255
 permit any
```

ACL Étendue (nommée)

```
ip access-list extended FILTRAGE-WEB
 permit tcp 192.168.10.0 0.0.0.255 any eq 80
 permit tcp 192.168.10.0 0.0.0.255 any eq 443
 deny   ip  192.168.10.0 0.0.0.255 any
 permit ip  any any
```

Appliquer une ACL sur une interface

```
interface GigabitEthernet0/1
 ip access-group FILTRAGE-WEB in    ! in  = trafic entrant sur l'interface
 ip access-group BLOC-VLAN30 out    ! out = trafic sortant de l'interface
```

Règles de placement

- ACL standard → placer au plus **près de la destination**
- ACL étendue → placer au plus **près de la source**

Vérification

```
show access-lists
show ip interface GigabitEthernet0/1   ! Montre les ACL appliquées
```

Une ACL se termine toujours par un `deny any` implicite. Toujours terminer par un `permit any` explicite si on veut autoriser le reste du trafic.

9. NAT / PAT

NAT statique (1 IP privée ↔ 1 IP publique fixe)

```
ip nat inside source static 192.168.1.10 203.0.113.10

interface GigabitEthernet0/0
 ip nat inside

interface GigabitEthernet0/1
 ip nat outside
```

PAT (NAT dynamique avec surcharge) — cas le plus courant

```
! Définir les IPs privées concernées
ip access-list standard NAT-POOL
 permit 192.168.0.0 0.0.255.255
```

```
! Activer le PAT sur l'interface WAN (utilise l'IP de l'interface)
ip nat inside source list NAT-POOL interface GigabitEthernet0/1 overload

! Marquer les interfaces
interface GigabitEthernet0/0
 ip nat inside

interface GigabitEthernet0/1
 ip nat outside
```

Vérification

```
show ip nat translations
show ip nat statistics
clear ip nat translation *            ! Vide la table NAT
```

10. Sécurisation des accès SSH

Étape 1 — Configurer le nom d'hôte et le domaine (obligatoires pour SSH)

```
hostname SW-CORE
ip domain-name monreseau.local
```

Étape 2 — Générer la paire de clés RSA

```
crypto key generate rsa modulus 2048
```

Étape 3 — Créer un utilisateur local

```
username admin privilege 15 secret MotDePasseFort!
```

Étape 4 — Configurer SSH v2

```
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3
```

Étape 5 — Configurer les lignes VTY

```
line vty 0 15
 transport input ssh         ! SSH uniquement (interdit Telnet)
 login local                 ! Authentification via base locale
 exec-timeout 10 0           ! Déconnexion après 10 min d'inactivité
```

Étape 6 — Sécuriser la console et désactiver Telnet

```
line console 0
 password MotDePasseConsole
 login
 exec-timeout 5 0

no service telnet             ! Désactive Telnet globalement si supporté
```

Vérification

```
show ip ssh
show ssh
show users                    ! Sessions actives
```

11. Sécurité complémentaire

Mot de passe enable chiffré

```
enable secret MotDePasseEnable!     ! Toujours utiliser secret et non
password
```

Chiffrement de tous les mots de passe en clair

```
service password-encryption
```

Bannière de connexion

```
banner motd # Acces reserve au personnel autorise. Toute connexion est
journalisee. #
```

Désactiver les services inutiles

```
no ip http server             ! Désactive l'interface web HTTP
no ip http secure-server      ! Désactive HTTPS (si non utilisé)
no cdp run                    ! Désactive CDP si non nécessaire
```